APPENDIX B TO PART 327—INTERNAL MANAGEMENT CONTROL REVIEW CHECKLIST

(a) *Task:* Personnel and/or Organization Management.

(b) *Subtask:* Privacy Act (PA) Program.

(c) *Organization:*

(d) *Action officer:*

(e) *Reviewer:*

(f) *Date completed:*

(g) *Assessable unit:* The assessable units are HQ, DeCA, Regions, Central Distribution Centers, Field Operating Activities, and commissaries. Each test question is annotated to indicate which organization(s) is (are) responsible for responding to the question(s). Assessable unit managers responsible for completing this checklist are shown in the DeCA, MCP, DeCA Directive 70–2.[1]

(h) *Event cycle 1:* Establish and implement a Privacy Act Program.

(1) Risk: If prescribed policies, procedures and responsibilities of the Privacy Act Program are not adhered to, sensitive private information on individuals can be given out to individuals.

(2) Control Objectives: The prescribed policies, procedures and responsibilities contained in 5 U.S.C. 552a are followed to protect individual privacy and information release.

(3) Control Techniques: 32 CFR part 310 and DeCA Directive 30–13,[2] Privacy Act Program.

(i) Ensure that a PA program is established and implemented.

(ii) Appoint an individual with PA responsibilities and ensure the designation of appropriate staff to assist.

(4) Test Questions: Explain rationale for YES responses or provide cross-references where rationale can be found. For NO responses, cross-reference to where corrective action plans can be found. If response is NA, explain rationale.

(i) Is a PA program established and implemented in DeCA to encompass procedures for subordinate activities? (DeCA HQ/SA, Region IM). Response: Yes / No / NA. Remarks:

(ii) Is an individual appointed PA responsibilities? (DeCA HQ/SA, Region IM). Response: Yes / No / NA. Remarks:

(iii) Are the current names and office telephone numbers furnished OSD, Private Act Office of the PA Officer and the IDA? (DeCA HQ/SA). Response: Yes / No / NA. Remarks:

(iv) Is the annual PA report prepared and forwarded to OSD, Defense Privacy Office? (DeCA HQ/SA). Response: Yes / No / NA. Remarks:

(v) Is PA awareness training/orientation provided? Is in-depth training provided for personnel involved in the establishment, development, custody, maintenance and use of a system of records? (DeCA HQ/SA, Region). Response: Yes / No / NA. Remarks:

(vi) Is the PA Officer consulted by information systems developers for privacy requirements which need to be included as part of the life cycle management of information consideration in information systems design? (DeCA HQ/SA, Region). Response: Yes / No / NA. Remarks:

(vii) Is each system of records maintained by DeCA supported by a Privacy Act System Notice and has the systems notice been published in the FEDERAL REGISTER? (DeCA HQ/SA). Response: Yes / No / NA. Remarks:

(i) *Event cycle 2:* Processing PA Requests.

(1) Risk: Failure to process PA requests correctly could result in privacy information being released which subjects the Department of Defense, DeCA or individuals to criminal penalties.

(2) Control Objective: PA requests are processed correctly.

(3) Control Technique:

(i) Ensure PA requests are logged into a formal control system.

(ii) Ensure PA requests are answered promptly and correctly.

(iii) Ensure DeCA records are only withheld when they fall under the general and specific exemptions of 5 U.S.C. 552a and one or more of the nine exemptions under DeCA Directive 30–12,[3] Freedom of Information Act (FOIA) Program.

(iv) Ensure all requests are coordinated through the General Counsel.

(v) Ensure all requests are denied by the DeCA IDA.

(vi) Ensure all appeals are forwarded to the Director DeCA or his designee.

(4) Test Questions:

(i) Are PA requests logged into a formal control system? (DeCA HQ/SA, Region IM). Response: Yes / No / NA. Remarks:

(ii) Are individual requests for access acknowledged within 10 working days after receipt? (DeCA HQ/SA, Region IM). Response: Yes / No / NA. Remarks:

(iii) when more than 10 working days are required to respond to a PA request, is the requester informed, explaining the circumstances for the delay and provided an approximate date for completion? (DeCA HQ/SA, Region IM). Response: Yes / No / NA. Remarks:

(iv) Are DeCA records withheld only when they fall under one or more of the general or specific exemptions of the PA or one or more of the nine exemptions of the FOIA? (DeCA HQ/SA, Region IM). Response: Yes / No / NA. Remarks:

[1] Copies may be obtained: Defense Commissary Agency, ATTN: FOIA/Privacy Officer, 1300 E. Avenue, Fort Lee, VA 23801–1800.

[2] See footnote 1 to this Appendix B.

[3] See footnote 1 to this Appendix B.

(v) Do denial letters contain the name and title or position of the official who made the determination, cite the exemption(s) on which the denial is based and advise the PA requester of their right to appeal the denial to the Director DeCA or designee? (DeCA HQ/SA). Response: Yes / No / NA. Remarks:

(vi) Are PA requests denied only by the HQ DeCA IDA? (All). Response: Yes/No/NA. Remarks:

(vii) Is coordination met with the General Counsel prior to forwarding a PA request to the IDA? (DeCA HQ/SA). Response: Yes/No/NA. Remarks:

(j) *Event cycle 3:* Requesting PA Information.

(1) Risk: Obtaining personal information resulting in a violation of the PA.

(2) Control Objective: Establish a system before data collection and storage to ensure no violation of the privacy of individuals.

(3) Control Technique: Ensure Privacy Act Statement to obtain personal information is furnished to individuals before data collection.

(4) Test Questions:

(i) Are all forms used to collect information about individuals which will be part of a system of records staffed with the PA Officer for correctness of the Privacy Act Statement? (DeCA HQ/SA, Region). Response: Yes/No/NA. Remarks:

(ii) Are Privacy Statements prepared and issued for all forms, formats and questionnaires that are subject to the PA, coordinated with the DeCA forms manager? (DeCA HQ/SA, Region). Response: Yes/No/NA. Remarks:

(iii) Do Privacy Act Statements furnished to individuals provide the following:

(A) The authority for the request.

(B) The principal purpose for which the information will be used.

(C) Any routine uses.

(D) The consequences of failing to provide the requested information. Yes/No/NA. Remarks:

(k) *Event cycle 4:* Records Maintenance.

(1) Risk: Unprotected records allowing individuals without a need to know access to privacy information.

(2) Control Objective: PA records are properly maintained throughout their life cycle.

(3) Control Technique: Ensure the prescribed policies and procedures are followed during the life cycle of information.

(4) Test Questions:

(i) Are file cabinets/containers that house PA records locked at all times to prevent unauthorized access? (All). Response: Yes/No/NA. Remarks:

(ii) Are personnel with job requirement (need to know) only allowed access to PA information? (All). Response: Yes/No/NA. Remarks:

(iii) Are privacy act records treated as unclassified records and designated 'For Official Use Only'? (All). Response: Yes/No/NA. Remarks:

(iv) Are computer printouts that contain privacy act information as well as disks, tapes and other media marked 'For Official Use Only'? (All). Response: Yes/No/NA. Remarks:

(v) Is a Systems Manager appointed for each automated/manual PA systems of records? (DeCA HQ/SA, Region). Response: Yes/No/NA. Remarks:

(vi) Are PA records maintained and disposed of in accordance with DeCA Directive 30–2,[4] The Defense Commissary Agency Filing System? (All). Response: Yes/No/NA. Remarks:

(l) I attest that the above listed internal controls provide reasonable assurance that DeCA resources are adequately safeguarded. I am satisfied that if the above controls are fully operational, the internal controls for this sub-task throughout DeCA are adequate.

Safety, Security and Administration.

FUNCTIONAL PROPONENT.

I have reviewed this sub-task within my organization and have supplemented the prescribed internal control review checklist when warranted by unique environmental circumstances. The controls prescribed in this checklist, as amended, are in place and operational for my organization (except for the weaknesses described in the attached plan, which includes schedules for correcting the weaknesses).

ASSESSABLE UNIT MANAGER (Signature).

APPENDIX C TO PART 327—DECA BLANKET ROUTINE USES

(a) *Routine Use—Law Enforcement.* If a system of records maintained by a DoD Component, to carry out its functions, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or by regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, the agency concerned, whether Federal, State, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.

(b) *Routine Use—Disclosure when Requesting Information.* A record from a system of records maintained by a Component may be disclosed as a routine use to a Federal, State, or local agency maintaining civil, criminal, or other relevant enforcement information or other pertinent information, such as current licenses, if necessary to obtain information relevant to a Component decision concerning the hiring or retention

[4] See footnote 2 to this Appendix B.